On the relation between the invariants of a doubly even self-dual binary code C and the invariants of the even unimodular lattice L(C) defined from the code C.(Algebraic Combinatorial Theory)

AUTHOR(S):

Ozeki, Michio

数理解析研究所講究録
671 巻 1988 年 126-138

On the relation between the invariants of a doubly even self-dual binary code C and the invariants of the even unimodular lattice L(C) defined from the code C.

弘前大理 小関道夫 (Michio Ozeki)

§1. Introduction

Let n be a natural number divisible by 4 and C a doubly even self-dual binary [2n,n] code. Furthermore we may assume that C is extremal. L(C) denotes the lattice defined from the code C by a modified Leech-Sloane construction. Here we give a sketchy description of L(C). Let f_i $(1 \leqq i \leqq 2n)$ be orthogonal vectors with the norm $(f_i,f_i)=2$, where $(\ ,\ )$ is the standard inner product in Euclidean space R^{2n}. We define vectors x satisfying the following conditions :

(i) $x = \frac{1}{2}(a_{i_1} f_{i_1} + \cdots\cdots + a_{i_r} f_{i_r})$,

(ii) $a_i = \pm 1$ for $i = i_1, i_2, \ldots, i_r$,

(iii) $\mathrm{supp}\, x = (x_1, \ldots\ldots, x_{2n}) \in C$,

where x_i is 1 if $i=i_1,\ldots,i_r$ and 0 otherwise,

(iv) $\prod_{k=1}^{r} a_{i_k} = 1$.

Note that r is divisible by 4 because C is doubly even.

Let M be the lattice generated by the vectors $\pm f_i \pm f_j$ ($1 \leqq i,j \leqq 2n$) over Z, the ring of rational integers. The lattice J is generated by M and the vectors x in the above form. We set

$$x_0 = \frac{1}{4}(f_1+f_2+\ldots+f_{2n-1} + \begin{cases} -3f_{2n} & \text{if } 2n \equiv 8 \pmod{16} \\ f_n & \text{if } 2n \equiv 0 \pmod{16} \end{cases}) .$$

Then L(C) is the lattice generated by J and the vector x_0. We can show that L(C) is an even unimodular extremal lattice of rank 2n when $8 \leqq 2n \leqq 40$. Indeed we know that

(a) if 2n=8, then C is the Hamming code H_8 and L(C) is the E_8 root lattice,

(b) if 2n=16, then C is the $H_8 \oplus H_8$ or d_{16} code and L(C) is the lattice containing D_{16} or $E_8 \oplus E_8$,

(c) if 2n =24, then C is the extended Golay code, and L(C) is the Leech lattice,

(d) if 2n=32, then C is each one of the five extremal codes

of length 32 (conf[1]) and L(C) is an extremal (unnamed) lattice,

(e) if 2n=40, then some examples of C are given in [3],[4] and [7] and L(C) are accounted in [5].

We now raise a fundamental problem

Problem (☆) Is the map $C \to L(C)$ injective ? Namely are the lattices $L(C_1)$ and $L(C_2)$ not isomorphic if the codes C_1 and C_2 are non-equivalent ?

One tool to treat this problem is theta-series $\theta_m(Z,L(C))$ of various degrees m. We give two examples for this.

Example 1. When 2n=32, we may prove that

for two binary self-dual [32,16,8] codes C_1 and C_2 , it holds that

$$\theta_1(z,L(C_1)) = \theta_1(z,L(C_2)), \qquad (1)$$

$$\theta_2(Z,L(C_1)) = \theta_2(Z,L(C_2)), \qquad (2)$$

$$\theta_3(Z,L(C_1)) = \theta_3(Z,L(C_2)), \qquad (3)$$

but

$$\theta_4(Z,L(C_1) \neq \theta_4(Z,L(C_2)) \qquad (4) .$$

The equalities (1),(2) and (3) can be proved with the help of [8],[9]. The inequality (4) is not yet proved, but the proof would not be much difficult. The underlying fact for this phenomenon would be that the codewords of fixed weight (8,...) of extremal binary[32,16] codes form a 3-design.

Example 2. When 2n=40, in [4] I gave three examples C_1, C_2 and C_3 of extremal codes. In [5] I showed that

$$\theta_1(z,L(C_i)) = \theta_1(z,L(C_j)) \quad i \neq j \ ,$$

$$\theta_2(Z,L(C_i)) \neq \theta_2(Z,L(C_j)) \quad .$$

In the same paper, I proposed a problem :

(☆☆) θ_2 distinguishes L(C) ?

Before the publication of the above paper [5], I remarked a paper by Iorgov [3], which treats the [40,20,8] codes. I examined the codes given by Iorgov along my method in [5]. And I found that my problem (☆☆) is not a good one. Neverthless, the problem (☆) seems to be valid. I will explain the detail in the next section.

§ 2. [40,20,8] codes and the derived lattices

Let C be a doubly even self-dual [40,20,8] code. O(C) de-

notes the set of all octads in C. By a theorem of Assumus-Mattson, O(C) forms a 1-design, and the cardinality of O(C) is 285. Let m be any number with $1 \leqq m \leqq 40$, then the number of octads in O(C) which take the value 1 at the m-th coordinate position is 57, independently of m. As in [5], we say that an octad v in O(C) passes through two coordinate positions (m,n) $(1 \leqq m < n \leqq 40)$ if v takes the value 1 at m-th and n-th coordinate positions. (in abbreviation c.p.). We define the index ind(m,n) for (m,n) by

$$\text{ind}(m,n) = \#\{v \in O(C) \mid v \text{ passes through } (m,n)\} .$$

We also define the supplementary index s-ind(m,n) and the half-index h-ind(m,n) for (m,n) by

$$\text{s-ind}(m,n) = \#\{v \in O(C) \mid v \text{ takes 0 at m-th and n-th c.p.}\}$$

$$\text{h-ind}(m,n) = \#\{v \in O(C) \mid \text{either } v \text{ takes 1 at m-th c.p. and 0 at n-th c.p. or 0 at m-th c.p. and 1 at n-th c.p.}\} .$$

The proof of the following lemma is found in [5].

Lemma 1. If ind(m,n)=q, then we have

$$\text{h-ind}(m,n) = 114-2q$$

$$\text{s-ind}(m,n) = 17l+q \quad .$$

We need another kind of invariants for the calculation of theta-series of degree 2. For a fixed octad v_0 in O(C), we define

$$\mu_j(v_0) = \#\left\{ u \in O(C) \mid u * v_0 = j \right\} ,$$

where $u * v_0$ is the number of common c.p. of u and v_0 which take the value 1. One may note that $\mu_j(v_0) \neq 0$ only when j=0,2,4 and 8. By virtue of Mendelsohn-Wilson equation for the design, we can obtain

$$\mu_2(v_0) = 224 - 2\mu_4(v_0)$$

and

$$\mu_0(v_0) = 60 + \mu_4(v_0) \quad .$$

Let M(2,k) be the space of Siegel modular forms of degree 2 and weght k.

It is known that

$$\dim M(2,20) = 5 \qquad (5)$$

and

$$\theta_2(Z,L(C)) \in M(2,20).$$

Since L(C) is an extremal lattice we know the set $\Lambda_2(L(C)) =$

$= \{ x \in L(C) \mid (x,x)=2 \}$ is an empty set. And we set

$$\Lambda_4(L(C)) = \{ x \in L(C) \mid (x,x)=4 \} .$$

Theta-series of degree 2 for L(C) $\theta_2(Z,L(C))$ is expanded to

$$\theta_2(Z,L(C)) = \sum_T a(T) e^{2\pi i \sigma(TZ)} ,$$

where $T = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ runs over all positive semi-definite semi-integral symmetric matrices of size 2 and σ is the trace of the matrix. a(T) is the number of pairs $<x,y>$ in $L(C) \times L(C)$ satisfying

$$(x,x) = 2a , \quad (x,y) = b, \quad (y,y) = 2c .$$

An easy computation shows that

$$a\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 1, \quad a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0 , \quad a\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = 39500 , \quad a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0.$$

If we can know one of $a\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $a\begin{pmatrix} 2 & 1/2 \\ 1/2 & 2 \end{pmatrix}$ or $a\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, then $\theta_2(Z,L(C))$ must be determined uniquely because of (5). For $x \in \Lambda_4(L(C))$ we define $\gamma_r(x) = \#\{ y \in \Lambda_4(L(C)) \mid (x,y)=r \}$ $r=0,1,2$, then we see that

$$a\begin{pmatrix} 2 & r/2 \\ r/2 & 2 \end{pmatrix} = \sum_{x \in \Lambda_4(L(C))} \gamma_r(x) .$$

The set $\Lambda_4(L(C))$ is divided into two subsets A and B :

$$\Lambda_4(L(C)) = A \cup B \qquad (A \cap B = \phi),$$

$$A = \left\{ \pm f_i \ \pm f_j \right\} \qquad 1 \leqq i < j \leqq 40 ,$$

$$B = \left\{ x \,\middle|\, x \text{ is a vector of the form (i) in §1 and supp } x \in O(C) \right\}.$$

The cardinalities of A and B are $4\times\binom{40}{2}=3120$ and $285\times 2^7=36480$ respectively. We call an x in A an α-type 4-vector and an x in B a β-type 4-vector. The following two lemmas are proved in [5].

Lemma 2. Let x be an α-type 4-vector, and $x=\pm f_m \pm f_n$, then we have

$$\nu_0(x) = 24702 + 192\ \mathrm{ind}(m,n) ,$$

$$\nu_1(x) = 7296 - 128\ \mathrm{ind}(m,n),$$

$$\nu_2(x) = 152 + 32\ \mathrm{ind}(m,n) .$$

Lemma 3. Let x be a β-type 4-vector and supp $x = u \in O(C)$, then we have

$$\begin{aligned}\nu_0(x) &= 2110 + 48\mu_4(u) + 64\mu_2(u) + 128\mu_0(u)\\ &= 24126 + 48\mu_4(u) ,\end{aligned}$$

$$\begin{aligned}\nu_1(x) &= 512 + 32\mu_4(u) + 32\mu_2(u)\\ &= 7680 - 32\mu_4(u) ,\end{aligned}$$

$$\nu_2(x) = 56 + 8\mu_4(u) .$$

In [4] I gave three [40,20,8] binary codes $C(NH_1)$, $C(NH_2)$ and $C(NH_3)$ ($C(NH_1)$ is well-known), and in [5] I examined the theta-series of degree 2 attached to the lattices $L_1=L(C(NH_1))$, $L_2=L(C(NH_2))$ and $L_3=L(C(NH_3))$. I computed the quantities $\nu_0(x)$, $\nu_1(x)$, $\nu_2(x)$ and determined $\theta_2(Z,L_i)$ $(i=1,2,3)$ that are mutually different. Later I became aware of a paper by Iorgov [3], and I examined the lattices derived from the codes in [3]. Here I give some values of $\mu_2(\text{supp }(x))$ $\nu_i(x)$ attached to the codes as tables. I utilize some of the notations in [3]. When x is an α-type 4-vector and $x=\pm f_m \pm f_n$, we write supp (x) to denote the coordinate positions (m,n).

Iorgov's code C_1, $L(C_1)$.

ind(supp (x))	$\nu_0(x)$	$\nu_1(x)$	$\nu_2(x)$	multiplicity	
7	26046	6400	376	2560	α-type
25	29502	4096	952	560	4-vector
μ_2(supp (x))	$\nu_0(x)$	$\nu_1(x)$	$\nu_2(x)$	multiplicity	
0	29502	4096	952	640=128 5	β-type
144	26046	6400	376	35840=128 280	4-vector

Iorgov's code C_2, $L(C_2)$

ind(supp (x))	$\nu_0(x)$	$\nu_1(x)$	$\nu_2(x)$	multiplicity	
7	26046	6400	376	2304	
13	27198	5632	568	448	α-type
25	29502	4096	952	336	4-vectpr
49	34110	1024	1720	32	
μ_2(supp (x))	$\nu_0(x)$	$\nu_1(x)$	$\nu_2(x)$	multiplicity	
0	29502	4096	952	384	
96	27198	5632	568	1792	β-type
144	26046	6400	376	32256	4-vector
168	25470	0784	280	2048	

Iorgov code C_4 , $L(C_4)$

ind(supp (x))	$\nu_0(x)$	$\nu_1(x)$	$\nu_2(x)$	multiplicity	
7	26046	6400	376	2048	
13	27198	5632	568	896	α-type
25	29502	4096	952	112	4-vector
49	34110	1024	1720	64	
μ_2(supp (x))	$\nu_0(x)$	$\nu_1(x)$	$\nu_2(x)$	multiplicity	
0	29502	4096	952	128	
96	27196	5632	568	3584	β-type
144	26046	6400	376	28672	4-vector
168	25470	6784	280	4096	

These values mean that their theta-series $\theta_2(Z,L)$ of degree coinside, contradictorily to the problem (☆☆). However the lattices are not isomorphic to each other, because the values $\nu_i(x)$ and

their multiplicities are isomorphism invariants for the lattice. In particular, the lattices $L(C_2)$ and $L(C_4)$ are barely distinguished by the multiplicities of the invariants. By the same token we can show that the lattices for the code $C(NH_2)$ and Iorgov's code C_5 have the identical theta-series of degree 2 but are not isomorphic.

Finally I give four concluding remarks for the present report.

Rem. 1. There are at least 11 non-isomorphic even unimodular extremal lattices of rank 40. Each of them is derived from a binary self-dual extremal [40,20] code.

Rem. 2. When we try to calculate the Fourier coefficients of theta-series of various degrees attached to the extremal lattices which come from binary or ternary extremal codes, we must face the various invariants of the codes similar to $\mu_2(\mathrm{supp}\ (x))$, ind(m,n) in the present report.

Rem. 3. It has now become clear that the problem (☆☆) is a ill-posed problem, but the problem (☆) is seemingly valid even now.

Rem. 4. The invariants like $\gamma_i(x)$ for the lattice would be finer invariants than theta-series of various degrees. But the former is more computational than the latter. Thus at present we can not see the structural beauty in the former.

References

[1] J.H.Conway and V.Pless, On the enumeration of self-dual codes, J. Comb. Th. Ser. A 28 (1980) 26-53.

[2] J.H.Conway and N.J.A.Sloane, Sphere-Packings, Lattices and Groups., New York : Springer-Verlag 1988.

[3] V.I.Iorgov, Binary self-dual codes with automorphisms of odd order, Problems of Information Transmission 19(1983) 260-270.

[4] M.Ozeki, Hadamard matrices and doubly even self-dual error-correcting codes, J.Comb. Th. Ser.A 44(1987) 274-287.

[5] M.Ozeki, Examples of even unimodular extremal lattices of rank 40 and their Siegel theta-series of degree 2, J. Number Th. 28(1988) 119-131.

[6] M.Ozeki, Ternary code constructions of even unimodular lattices, to appear in the Proceedings of International Num. Th. Conf. held at Quebec 1987

[7] V.D.Tonchev, Hadamard-type block designs and self-dual codes, Problems of Information Transmission 19(1983) 270-274.

[8] S.Tsuyumine, On Siegel modular forms of degree three, Amer.

J. Math. 108(1986) 755-862.

[9] B.B.Venkov, On even unimodular Euclidean lattices of dimension 32, J. Soviet Math. 26 (1984) 1860-1867.